[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
B60R 25/04
G06F 12/16 F02D 45/00

[12]发明专利申请公开说明书

[21]申请号 01111611.0

[43]公开日 2001年10月3日

[11]公开号 CN 1315275A

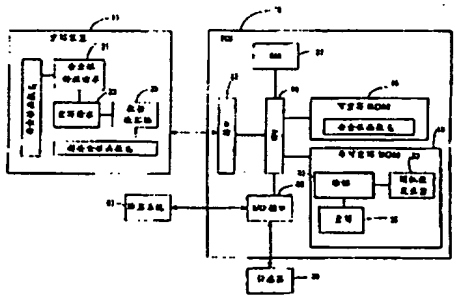
[22]申请日 2001.3.16 [21]申请号 01111611.0
[30]优先权
[32]2000.3.16 [33]JP [31]074236/2000
[71]申请人 本田技研工业株式会社
地址 日本东京都
[72]发明人 屋敷哲也 松浦正典 水尾直彦
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 王茂华

权利要求书4页 说明书12页 附图页数9页

[54]发明名称 用于车辆控制器的存储器重写系统

[57]摘要

一种用于一个车辆控制器的存储器重写系统，包括车辆控制器和外部重写装置。车辆控制器包括一个存储第一安全性数据的可重写存储器。第一安全性数据用来确定是否允许对可重写存储器重写。重写装置把新安全性数据传送到车辆控制器。车辆控制器删除第一安全性数据，并且把新安全性数据写入可重写存储器中。重写新安全性数据由存储在一个非可重写存储器中的一个程序进行。



ISSN1008-4274

权 利 要 求 书

1.一种车辆控制器，包括一个用来存储用于确定是否允许对可重写存储器重写的第一安全性数据的可重写存储器；

其中把车辆控制器配置成，响应来自一个外部重写装置的新安全性数据的接收，删除第一安全性数据、和把新安全性数据写入可重写存储器中。

2.根据权利要求 1 所述的车辆控制器，其中用来删除第一安全性数据和写新安全性数据的程序存储在一个非易失性存储器中。

3.根据权利要求 1 所述的车辆控制器，其中防盗系统连接到车辆控制器上；及

其中如果防盗系统允许关于车辆的操作，则允许对可重写存储器的重写。

4.根据权利要求 1 所述的车辆控制器，其中以闪烁存储器、EPROM、和 EEPROM 的任何形式实现可重写存储器。

5.根据权利要求 2 所述的车辆控制器，其中以单个存储器的形式实现可重写存储器和非可重写存储器。

6.一种重写装置，用来重写包括在一个车辆控制器中的一个可重写存储器；

一个存储器，用来存储新安全性数据；

一个通信装置，用来传送新安全性数据，以把新安全性数据写入可重写存储器中；及

其中写入可重写存储器中的安全性数据用来确定是否允许对可重写存储器重写。

7.根据权利要求 6 所述的重写装置，其中可重写存储器存储用于确定是否允许对可重写存储器的重写的第一安全性数据；及

重写装置请求车辆控制器删除第一安全性数据、和把传送的新安全性数据写入可重写存储器中。

8.根据权利要求 6 所述的重写装置，进一步包括一个使用户能够

建立新安全性数据的用户接口。

9.根据权利要求 6 所述的重写装置，其中把控制器进一步配置成汇编来自新安全性数据的串行数据块；及

其中通信装置通过串行通信传送串行数据块。

10.一种用于车辆控制器的存储器重写系统，包括：

一个可重写存储器，安装在车辆控制器上，可重写存储器存储第一安全性数据，第一安全性数据用来确定是否允许对可重写存储器的重写；

一个重写装置，用来把新安全性数据传送到车辆控制器；及

其中把车辆控制器配置成删除第一安全性数据、和把新安全性数据写入可重写存储器中。

11.根据权利要求 10 所述的存储器重写系统，其中用来删除第一安全性数据和用来写新安全性数据的程序存储在一个非可重写存储器中。

12.根据权利要求 10 所述的存储器重写系统，其中使用重写装置任意建立新安全性数据。

13.根据权利要求 10 所述的存储器重写系统，其中一个防盗系统连接到车辆控制器上；及

其中如果防盗系统允许关于车辆的操作，则允许对可重写存储器的重写。

14.根据权利要求 10 所述的存储器重写系统，

其中重写装置存储第二安全性数据；及

把车辆控制器配置成把第一安全性数据与从重写装置传送的第二安全性数据相比较，并且如果第一安全性数据与第二安全性数据相匹配则允许对可重写存储器重写。

15.根据权利要求 10 所述的存储器重写系统，其中第一安全性数据和第二安全性数据具有相同的函数；

重写装置包括一个程序，以便根据第一安全性数据的函数对一个数计算一个第一函数值；及

把车辆控制器配置成，根据第二安全性数据的函数对于该数计算一个第二函数值、把第一函数值与从重写装置传送的第二函数值相比较、及如果第一函数值等于第二函数值则允许重写装置对可重写存储器重写。

16.根据权利要求 15 所述的存储器重写系统，其中该数在车辆控制器中从随机数产生，并且把该数从车辆控制器传送到重写装置。

17.根据权利要求 10 所述的存储器重写系统，其中经串行通信传送新安全性数据。

18.一种用来重写在车辆控制器中的可重写存储器中存储的数据的方法，该方法包括:

接收从一个外部重写装置传送到车辆控制器的新安全性数据;

删除存储在可重写存储器中的第一安全性数据，第一安全性数据用来确定是否允许对可重写存储器的重写；及

把新安全性数据写入可重写存储器中。

19.根据权利要求 18 所述的方法，其中由在安装在车辆控制器上的一个可重写存储器中存储的程序，进行删除第一安全性数据和写新安全性数据。

20.根据权利要求 18 所述的方法，其中防盗系统连接到车辆控制器上；及

其中如果防盗系统允许关于车辆的操作，则允许对可重写存储器的重写。

21.根据权利要求 18 所述的方法，

其中重写装置存储第二安全性数据；及允许对可重写存储器的重写的确定包括:

把第一安全性数据与从重写装置传送的第二安全性数据相比较;

如果第一安全性数据与第二安全性数据相匹配，则允许对可重写存储器的重写。

22.根据权利要求 21 所述的方法，其中第一安全性数据和第二安

全性数据具有相同的函数;

其中允许对可重写存储器的重写的确定包括:

根据在车辆控制器中的第一安全性数据的函数对一个数计算一个第一函数值;

根据在可重写装置中的第二安全性数据的函数对该数计算一个第二函数值;

把第一函数值与第二函数值相比较; 及

如果第一函数值等于第二函数值, 则允许重写装置对可重写存储器的重写。

01.03.16

说　　明　　书

用于车辆控制器的存储器重写系统

本发明涉及一种借助于从外部重写装置传送的另一种数据来重写存储在车辆控制器的存储器中的数据的存储器重写系统。

车辆经受通过一个电子控制单元(下文称作“ECU”)的各种类型的控制。这样的控制包括用于空气燃料比率、燃料喷射量、和排放的发动机相关控制；以及用于动力窗户、气囊、和ABS的车体有关控制。ECU根据由安装在车辆上的各种传感器检测的当前条件和车辆行驶状态，提供对车辆的各种类型控制。

另一方面，车辆可以包括一个防盗系统。一般地说，防盗系统电子检查由驾驶员用来启动发动机的点火钥匙是否是真的。如果确定钥匙是真的，则防盗系统把一个用来允许车辆操作的信号传送到ECU. 另一方面，如果确定点火钥匙不是真的，则判断驾驶员不是授权人，并且他不能操作车辆。因而，在接收到允许信号以前，ECU通过例如停止燃料喷射不允许发动机启动。

ECU包括一个中央处理单元(CPU)、一个存储要完成的程序和数据的ROM(只读存储器)、一个为执行提供工作区域和存储计算结果的RAM(随机存取存储器)、及一个用来从各传感器接收信号和把控制信号传送到发动机各部分的I/O接口。

ROM常常包括一个诸如闪烁存储器、一个EEPROM、或一个EPROM之类的可重写存储器，以允许在其中重写程序或数据。日本专利申请公开No. 63-223901描述了一种借助于安装在车辆上的ECU响应来自外部装置的请求来改变存储在ECU的EEPROM中的程序的方法。

改变存储在ECU的ROM中的程序或数据的这样一种功能，使得有必要保护程序或数据免于由外部装置存取，因而防止用户或其他第三方没有适当授权而重写存储在ROM中的程序或数据。日本

专利申请公开 No. 3-238541 描述了一种使用一个检查数据机构来确定在 ECU 的 ROM 中的程序或数据是否被篡改的车辆控制器。根据该机构，事先存储基于存储在 ROM 中的数据的检查数据。在车辆装运之后，ECU 根据存储在 ROM 中的数据建立新的检查数据。ECU 然后把新的检查数据与以前存储的检查数据相比较，如果他们不相同就确定数据已经被篡改数据并且接通报警灯。

用来释放上述安全特性的密钥仅对于在与汽车制造商的合同下的重写装置制造商是已知的。因而，只有由汽车制造商授权的重写装置能使用“密钥”和改变存储在该汽车 ECU 的 ROM 中的数据。

将简要描述用来改变 ROM 中的程序的一种典型过程。上述密钥一般由某一函数表示，该函数既提供在重写装置中又提供在 ECU 中。重写装置被连接到 ECU 上，并且然后使用其自己的函数(即密钥)对于从 ECU 传送的一个任意数字值计算一个函数值。重写装置然后把该函数值传送到 ECU。同时，ECU 使用其自己的函数(即密钥)对于相同的数字值计算一个函数值。ECU 把从重写装置接收的函数值与由其本身确定的函数值相比较。如果他们相等，则 ECU 释放安全特性。因而，允许重写装置重写存储在 ROM 中的数据。如果他们不相等，那么判断该重写装置不是真的，因为重写装置和 ECU 具有不同的函数(密钥)。因此，不释放安全特性，并且重写装置不能重写存储在 ROM 中的数据。

然而，用来释放安全特性的密钥按常规存储在 ECU 中的 ROM 的不可重写区域中，从而在车辆已经装运之后，不可能用重写装置改变密钥。因而，如果密钥偶然泄密到用户或没有授权的另外第三方，则除授权的之外的重写装置能重写 ROM 中的密钥，由此破坏安全特性。

另一方面，如果车辆包括一个防盗系统，并且如果重写用来操作防盗系统的程序，那么会使防盗系统失效。因而，用来重写存储在 ROM 中的程序或数据的系统需要比防盗系统高的安全性。

本发明的一个目的在于提供一种用于车辆控制器的存储器重写

系统，该存储器重写系统即使在车辆装运之后，也能改变用来释放防止存储在 ECU 的 ROM 中的程序或数据被篡改的安全特性的密钥。即使密钥已经泄密到没有授权的第三方，制造商也能使用该重写装置改变密钥，由此能够使安全特性容易地恢复。

本发明的另一个目的在于提供一种用于车辆控制器的存储器重写系统，该存储器重写系统能与防盗系统一起操作。

根据本发明的一个方面，提供一种包括一个可重写存储器的车辆控制器。可重写存储器存储用来确定是否允许对可重写存储器重写的第一安全性数据。把车辆控制器配置成，响应来自一个外部重写装置的新安全性数据的接收，删除第一安全性数据、和把新安全性数据写入可重写存储器中。可重写存储器能在诸如闪烁存储器、EPROM、和 EEPROM 之类的非易失性存储器中实现。因而，通过重写存储在可重写存储器中的安全性数据能容易地恢复安全特性，即使安全性数据已经泄密到第三方也防止非法重写扩散。

在本发明的一个实施例中，车辆控制器也包括一个非可重写存储器，其中存储用来删除第一安全性数据并且写入新安全性数据的程序。因而，防止重写安全性数据的程序免于被篡改。

在本发明的另一个实施例中，在单个存储器中实现可重写存储器和非可重写存储器。

在本发明的另一个实施例中，把一个防盗系统连接到车辆控制器上。在这种情况下，如果防盗系统允许关于车辆的操作，则允许对可重写存储器的重写。

根据本发明的另一个方面，提供一种用来重写包括在一个车辆控制器中的可重写存储器的重写装置。重写装置包括一个用来存储新安全性数据的存储器和一个用来传送新安全性数据的通信装置。把传送的新安全性数据写入可重写存储器中。写入可重写存储器中的安全性数据用来确定是否允许对可重写存储器重写。重写装置提供一个使用户能够建立新安全性数据的用户接口。况且，控制器能汇编来自新安全性数据的数据块。每个数据块包括一个用于新安全

性数据的部分程序代码的程序代码字段、和一个用于其中存储部分程序代码的可重写存储器的前导地址的地址字段。通信装置通过串行通信传送数据块。

在本发明的一个实施例中，重写装置进一步向车辆控制器发送一个请求，以删除第一安全性数据和把传送的新安全性数据写入可重写存储器中。

根据本发明的另一个方面，重写装置存储第二安全性数据。车辆控制器把在其中安装的可重写存储器中存储的第一安全性数据与从重写装置传送的第二安全性数据相比较。如果第一安全性数据与第二安全性数据相匹配，则车辆控制器允许重写装置对可重写存储器重写。

在本发明的一个实施例中，第一安全性数据和第二安全性数据具有相同的函数。重写装置包括一个程序，以便根据第一安全性数据的函数对一个数计算一个第一函数值。车辆控制器根据第二安全性数据的函数对于该数计算一个第二函数值。车辆控制器把第一函数值与从重写装置传送的第二函数值相比较。如果第一函数值等于第二函数值，则车辆控制器允许重写装置对可重写存储器重写.

图 1 表示根据本发明一个实施例的一种存储器重写系统的外观;

图 2 是方块图，表示根据本发明一个实施例的整个存储器重写系统;

图 3 表示在根据本发明一个实施例的存储器重写系统中的 ECU 的一个 ROM 和一个 CPU 的形式的例子;

图 4 表示根据本发明一个实施例的存储器重写系统的操作过程;

图 5 是由根据本发明一个实施例的存储器重写系统执行的一个验证过程;

图 6 是流程图，表示由根据本发明一个实施例的存储器重写系统执行的一个用来释放安全性的过程;

图 7 是流程图，表示由根据本发明一个实施例的存储器重写系统的 ECU 执行的一个用来释放安全性的过程；

图 8 是流程图，表示由根据本发明一个实施例的存储器重写系统的重写装置执行的一个用来重写的过程；及

图 9 是流程图，表示由根据本发明一个实施例的存储器重写系统的 ECU 执行的一个用来重写的过程。

参照附图将描述用来重写存储在车辆控制器的非易失性存储器中的安全性程序的本发明。然而，本发明不限于用来重写安全性程序的系统，而是适用于用来重写存储在一个非易失性存储存储器中的数据的各种系统。

图 1 表示根据本发明一个实施例的一种存储器重写系统的外观。存储器重写系统包括一个安装在一个车辆 1 上的电子控制单元 (ECU) 10 和一个重写装置 11。重写装置 11 由车辆 1 的制造商授权。ECU 10 包括一个可重写 ROM (未表示)。如图中所示，当把重写装置 11 连接到 ECU 10 上，并且进行对于重写装置 11 的一些适当操作时，释放用来防止存储在 ECU 10 的 ROM 中的程序或数据免于没有适当授权而被重写的安全特性。因而，允许重写装置重写存储在 ROM 中的程序或数据。

通过在 ECU 10 与重写装置 11 之间的串行通信执行重写。用户通过操作在重写装置 11 上的操作按钮和/或与提供在重写装置 11 上的显示屏幕交互作用，能把用来重写的数据发送到 ECU 10。然而，重写装置不限图中所示的形式，而是可以是具有能够与 ECU 10 通信的协议的另一种形式。

图 2 是功能方块图，表示根据本发明一个实施例的整个存储器重写系统。如上所述，存储器重写系统包括安装在车辆上的 ECU 10 和重写装置 11。重写装置 11 提供在 ECU 10 外面，并且经串行通信连接到其上。可选择地，在重写装置 11 与 ECU 10 之间可以使用并行通信。

ECU 10 包括：一个中央处理单元 14(下文称作 CPU)，包括一个

微型计算机和有关的电路元件；ROM 16 和 18，他们是非易失性存储器并且存储程序和数据；一个 RAM 37 (随机存取存储器)，为执行提供工作区域，并且存储计算结果；及一个 I/O 接口 38，用来从各传感器 39 接收信号和把控制信号传送到发动机的各部分。来自各传感器 39 的信号包括发动机转动速度(Ne)、发动机水温(Tw)、吸入空气温度(Ta)、电池电压(VB)、及点火开关(IGSW)。因而，根据从 I/O 接口 38 输入的一个信号，CPU 14 从 ROM 16 和 18 调用一个控制程序和数据以执行计算，并且经 I/O 接口 38 把结果输出到车辆的各部分以控制车辆的各种功能。

ECU 10 也包括一个接口 12。接口 12 带有用来与重写装置 11 通信的协议，以便在 ECU 10 与重写装置 11 之间能够实现串行通信。

可重写 ROM 16 是一个从其能删除存储数据和对其能写新数据的存储器。可重写 ROM 16 例如能是闪烁存储器或 EEPROM。通过把可重写 ROM 的存储器区域的一部分指定为不可改变区域、或通过使用对其在制造期间固化数据且以后不能从其删除或对其写数据的掩模 ROM，能实现非可重写 ROM 18。可选择地，借助于对其仅能写一次数据的一个 PROM 能实现 ROM 18。

ROM 16 和 18 能作为物理分离的两个存储器实现。另外，可以把单个存储器的存储器区域划分成两个区域，从而区域之一用作可重写区域，而其他用作非可重写区域。在后一种情况下，例如，在 EEPROM 中已经指定其中存储程序等的一个非可重写区域之后，在存储器的未填充空间中借助于一个开始地址和一个结束地址指定一个可重写区域。

现在，参照图 3 描述 ROM 16 和 18 及 CPU 的一种形式的例子。在该图中，ROM 16 和 18 使用一个闪烁存储器实现。图 3 (a)表示与 CPU 分离地提供闪烁存储器的一种形式。当通过与重写装置 11 的通信输入重写操作模式时，CPU 从重写装置 11 接收数据，并且借助于接收的数据调用用来重写闪烁存储器的一个程序。

另一方面，图 3(b)表示具有一个与 CPU 结合构成一个芯片的内

装闪烁存储器的一种形式。当响应来自重写装置的一个信号进入重写操作模式时，使用包括在 CPU 中的功能从重写装置传送的数据自动重写到该闪烁存储器。根据本发明的存储器重写装置适用于以上形式的任一种。

再参照图 2，可重写 ROM 16 存储一个安全性函数 f_2。安全性函数 f_2 实现用来防止存储在 ROM 16 中的数据被非法重写的安全特性。

非可重写 ROM 18 存储用来实现一个验证部分 31、一个随机数发生器 33、及一个重写部分 35 的程序。验证部分 31 响应用来从重写装置 11 释放安全性的请求，并且使用安全性函数 f_2 和由随机数发生器 33 产生的一个随机数 R 确定重写装置 11 是否是真的。使用随机数 R 能够实现要提高的安全特性。如果确定重写装置是真的，则验证部分 31 释放安全持性。

此后，重写部分 35 删除安全性函数 f_2，并且从重写装置 11 接收一个新的安全性函数 f_3，以把它重写到 ROM 16 中。安全性函数 f_2 可以物理或逻辑地删除。逻辑删除可以使用一个删除标志实现。更具体地说，带设置的删除标志的安全性函数 f_2 认为在以后的过程中删除。

重写装置 11 带有一个安全性函数 f_1 和一个新的安全性函数 f_3。安全性函数 f_1 和存储在 ECU 10 的 ROM 16 中的安全性函数 f_2 合作实现安全特性。如果安全性函数 f_2 没有由任何第三人改变，则重写装置 11 的安全性函数 f_1 与 ECU 10 的安全性函数 f_2 相同。在另一个实施例中，安全性函数 f_1 和 f_2 具有一定的关系。如果该关系保持，则确定安全性函数 f_2 没有被篡改。

在重写存储在 ROM 16 中的安全性函数 f_2 之前准备新的安全性函数 f_3。新的安全性函数 f_3 能通过对当前安全性函数 f_1 进行一些变化建立。根据一个例子，新的安全性函数 f_3 是一个与安全性函数 f_1 具有不同表达式的函数。根据另一个例子，新的安全性函数 f_3 是一个在函数表达式中具有与安全性函数 f_1 不同的常数的函数。例如，

当函数 f_1 和 f_2 是 $f_1=f_2=A\times R+B$ (A=10 和 B=5)时，把新的安全性函数 f_3 设置成 $f_3=A+R\times B$ (A=10 和 B=5)。可选择地，可以把函数 f_1 和 f_2 的常数 A 和 B 的值分别改变到 5 和 10。

重写装置 11 也包括一个安全性释放请求部分 21、一个重写请求部分 23、及一个数据块汇编部分 25，这些可以作为程序存储在重写装置 11 的一个存储器中。安全性释放请求部分 21 使用安全性函数 f_1 请求 ECU 10 释放安全特性。

数据块汇编部分 25 从安全性函数 f_3 的程序代码汇编适用于串行通信的数据块。每个数据块包括一个地址字段和一个程序代码字段。程序代码字段包含一个部分程序代码，而地址字段包含一个其中存储部分程序代码的区域的前导地址。数据块汇编部分 25 把安全性函数 f_3 的程序代码划分成多片，其每一片具有一定的长度(例如 8 位)。程序代码的每片或每个部分程序代码，放置在一个数据块的程序代码字段中。每个部分程序代码的一个前导地址放置在数据块的地址字段中。因而，汇编数据块。

在已经释放安全特性之后，重写请求部分 23 串行地把表示由数据块汇编部分 25 汇编的新安全性函数 f_3 的数据块传送到 ECU 10。

一个防盗系统 81 连接到 ECU 10 上，从而存储器重写系统能与防盗系统 81 交换信息。防盗系统 81 从当发动机要启动时插入在一个钥匙孔内的点火钥匙抽取一个电子代码，并且把该电子代码与一个预定授权代码相比较，以检查插入的点火钥匙是否是真的。如果确定点火钥匙是真的，则防盗系统 81 经一个 I/O 接口 38 把一个指示允许发动机启动的信号传送到 ECU 10。在接收到该允许信号时，ECU 10 设置可以存储在 RAM 37 或 ROM 16 中的发动机启动允许标志，并且启动发动机。如果确定插入的点火钥匙不是真的，则不输出允许信号。因而，ECU 10 不能启动发动机。尽管防盗系统 81 和 ECU 10 分别表示在图 2 中，但防盗系统 81 的一些功能可以包括在 ECU 10 中。例如，点火钥匙的授权可以由 ECU 10 完成。

参照图 4 和 5 描述表示在图 2 中的存储器重写系统的操作。例

如，当在把重写装置 11 已经连接到 ECU 10 上之后按下重写装置 11 的操作按钮时，开始重写操作。可选择地，重写操作可以通过操作 ECU 10 开始。

在步骤 41，重写装置 11 的安全性释放请求部分 21 把一个指示用于释放安全性请求的信号传送到 ECU 10。ECU 10 响应该信号启动一个验证过程，以便证实授权重写装置连接到其上。下面参照图 5 将描述验证过程。

如果 ECU 验证重写装置 11，并且允许它对可重写 ROM 16 重写，则过程前进到步骤 42。重写装置 11 的重写请求部分 23 把一个指示重写开始的信号传送到 ECU 10，并且当准备重写时，ECU 10 的重写部分 35 返回一个开始允许信号。在步骤 43，重写装置 11 把一个用来转移到一个重写操作模式的请求传送到 ECU 10，并且然后 ECU 10 的重写部分 35 执行一个用来转移到重写操作模式的过程。在步骤 44，重写请求部分 23 询问 ECU 10 是否已经完成操作模式的转移。如果已经完成转移，则重写部分 35 把一个指示转移完成的信号传送到重写装置 11。

在步骤 45，重写请求部分 23 请求删除存储在可重写 ROM 16 中的安全性函数 f_2，并且响应这点，重写部分 35 从 ROM 16 删除安全性函数 f_2。

在这时，在重写装置 11 中，已经准备新的安全性函数 f_3。函数 f_3 已经由数据块汇编部分 25 提供，作为用于传送到 ECU 10 的串行数据块。一般在重写装置 11 把用来释放安全性或通知重写开始的请求传送到 ECU 10 之前，建立安全性函数 f_3。然而，对于新安全性函数 f_3 的这种准备可以在步骤 45 之前立即执行。

可以准备新安全性函数 f_3，例如从以前保存在重写装置 11 中的多个函数选择一个。可选择地，用户可以通过操纵重写装置 11 建立新安全性函数 f_3。

在步骤 46，重写请求部分 23 把表示新安全性函数 f_3 的数据块的第一个与指示请求对可重写 ROM 16 重写的一个信号一起传送到

ECU 10. 重写部分 35 从重写装置 11 接收数据块，并且把包括在数据块中的一个部分程序代码写到可重写 ROM 16. 把部分程序代码写入由数据块的地址字段指示的一个地址中。一旦已经完成部分程序代码的写，重写部分 35 就把写完成的通知传送到重写装置 11. 作为对此的响应，重写装置 11 把下一个数据块传送到 ECU 10. 重复该步骤 46，直到把安全性函数 f_3 的所有程序代码写入到 ROM 16 中。

一旦已经完成所有程序代码的写，重写请求部分 23 就把一个用来释放重写操作模式的请求传送到 ECU 10 (步骤 47). 作为对此的响应，重写部分 35 释放重写操作模式。由于重写装置 11 已经把存储在 ROM 16 中的安全性函数变化到 f_3，所以把由重写装置 11 使用的函数也设置到 f_3，从而以后借助于安全性函数 f_3 能实现安全特性。在把新安全性函数 f_3 已经写到 ROM 16 之后，可以删除以前的安全性函数 f_1。

图 5 表示与图 4 中步骤 41 相对应的验证过程的一个例子. 在步骤 51，重写装置 11 的安全性释放请求部分 21 请求 ECU 10 传送一个任意数 R. 作为对此的响应，调用 ECU 10 的验证部分 31. 验证部分 31 调用产生随机数的随机数发生器 33. 验证部分 31 从由随机数发生器 33 产生的随机数选择数 R，并且把数 R 传送到重写装置 11(步骤 52). 可选择地，可以使用一个不同的机构来设置任意数 R. 重写装置 11 使用已经存储在其中的安全性函数 f_1，以便根据 $K1=f_1(R)$对于数据 R 确定函数 f_1 的函数值 K1 (步骤 53).

另一方面，ECU 10 的验证部分 31 使用存储在可重写 ROM 16 中的安全性函数 f_2，以便根据 $K2=f_2(R)$对于数 R 确定一个函数值 K2 (步骤 54). 重写装置 11 的安全性释放请求部分 21 把函数值 K1 传送到 ECU 10(步骤 55). 验证部分 31 把来自重写装置 11 的函数值 K1 与内部确定的函数值 K2 相比较 (步骤 56)，并且如果他们相等，则确定重写装置 11 是真的。以后，验证部分 31 检查存储在 RAM 37 中的发动机启动允许标志是否是值一 (步骤 57). 如果允许标志是

一，则这意味着已经从防盗系统 81 输出了发动机启动允许信号，并且把一个指示重写允许的信号传送到重写装置 11 (步骤 58).

因而，安全特性需要释放以便重写存储在可重写 ROM 中的数据，从而使用当前安全性函数 f_1 和 f_2 用来释放安全特性。借助于安装在车辆中的防盗系统，只有已经释放了防盗系统，才释放用于存储器重写系统的安全特性，由此防止非法驾驶员重写数据。

图 6 是流程图，表示由存储器重写装置 11 执行的一个用来释放安全性的过程。在步骤 61，重写装置 11 从 ECU 10 请求一个数 R。重写装置 11 以后从 ECU 10 接收数 R (步骤 62)。在接收到数 R 时，重写装置 11 使用已经保持在其中的安全性函数 f_1 对于数 R 计算函数值 K1 (步骤 63)。以后，重写装置 11 把函数值 K1 传送到 ECU 10 (步骤 64)。

图 7 是流程图，表示由 ECU 10 执行的一个用来释放安全性的过程。ECU 10 从重写装置 11 接收对于数 R 的请求。在接收到该请求时，ECU 10 设置来自随机数的数 R (步骤 72)，并且把它传送到重写装置 11 (步骤 73)。ECU 然后使用已经保持在其中的安全性函数 f_2 对于数 R 计算函数值 K2 (步骤 74).

ECU 10 从重写装置 11 接收函数值 K1(步骤 75)，并且把值 K1 与值 K2 相比较 (步骤 74)。如果他们相等，则 ECU 10 检查发动机启动允许标志是否是一(步骤 77)。如果标志是一，则过程前进到步骤 78 以设置一个重写允许标志，由此指示允许重写装置 11 重写。如果在步骤 76 值不相等，或者在步骤 77 没有把发动机启动允许标志设置到值一，那么把重写允许标志设置到零(步骤 79)，以指示不允许重写装置重写。

图 8 是流程图，表示重写装置 11 执行的一个用来重写的过程。在步骤 81，重写装置 11 传送用来重写到 ECU 10 的请求。该请求实际可以包括表示在图 4 中的用于重写开始的通知、用来转移到重写操作模式的请求等。在响应用来重写的请求接收由 ECU 10 提供的重写允许时(步骤 82)，重写装置 11 建立新安全性函数 f_3 的数据块(步骤

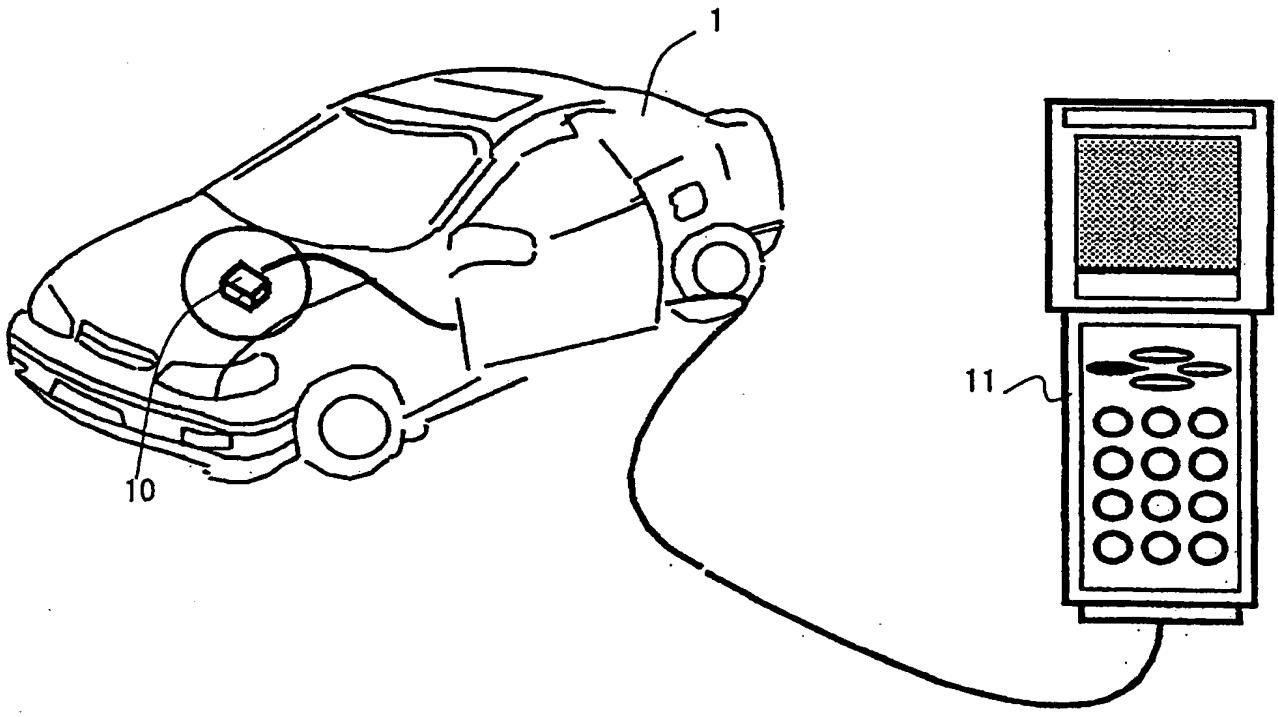
83)。使用上述的重写装置 11 能任意建立新安全性函数 f_3。重写装置 11 然后把表示新安全性函数 f_3 的数据块传送到 ECU 10 (步骤 84)。

图 9 是流程图，表示由 ECU 10 执行的一个用来重写的过程。在从重写装置 11 接收到用来重写的请求时(步骤 91)，ECU 10 检查把重写允许标志是否设置到一(步骤 92)。如果把标志设置到一，这意味着已经证明重写装置 11 是真的，那么 ECU 等待从重写装置 11 传送的新安全性函数 f_3。事实上，在步骤 92 与 93 之间能执行诸过程，如图 4 中所示的至重写操作模式的转移或从可重写 ROM 删除当前安全性函数 f_2。

以后，在接收到新安全性函数 f_3 时(步骤 93)时，ECU 把该函数 f_3 写到可重写 ROM 16。因而，借助于新安全性函数 f_3 重写已经存储在可重写 ROM 16 中的安全性函数 f_2。

说 明 书 附 图

图1



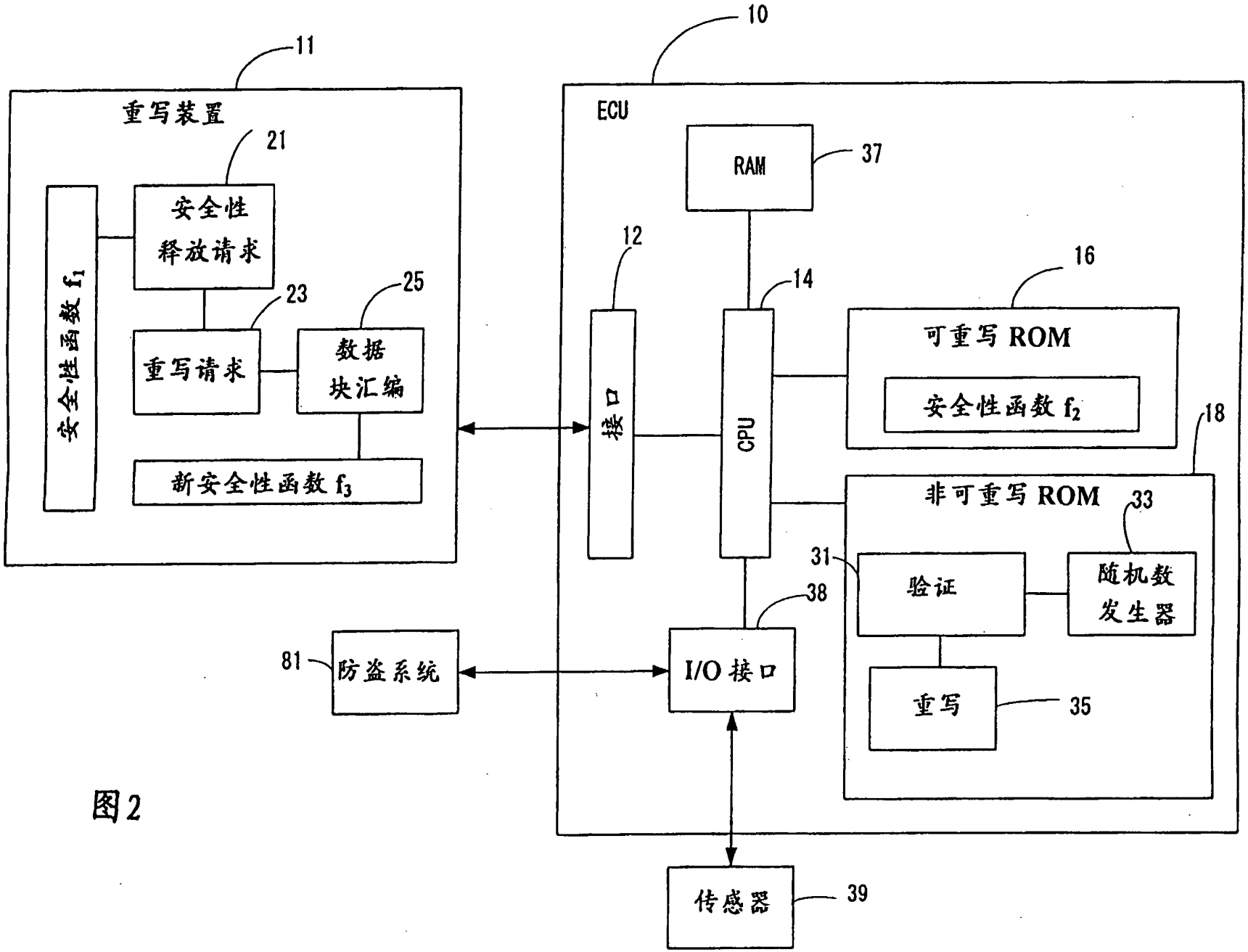

10
11
重写装置
21
安全性
释放请求
安全性函数 f_1
23
重写请求
25
数据
块汇编
新安全性函数 f_3
ECU
RAM
37
12
14
16
接口
CPU
可重写 ROM
安全性函数 f_2
18
非可重写 ROM
33
31
验证
随机数
发生器
38
81
防盗系统
I/O 接口
重写
35
传感器
39

图2

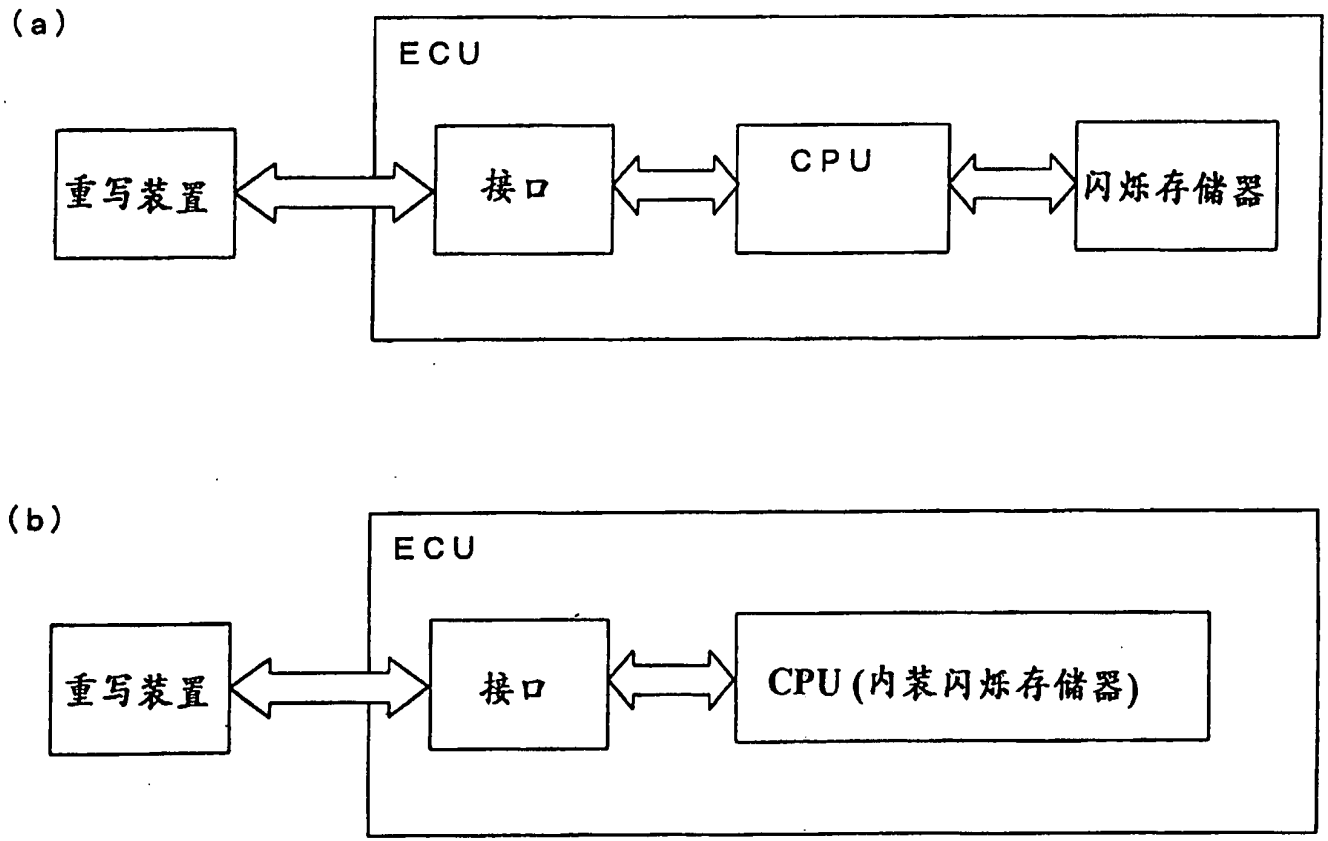


图3

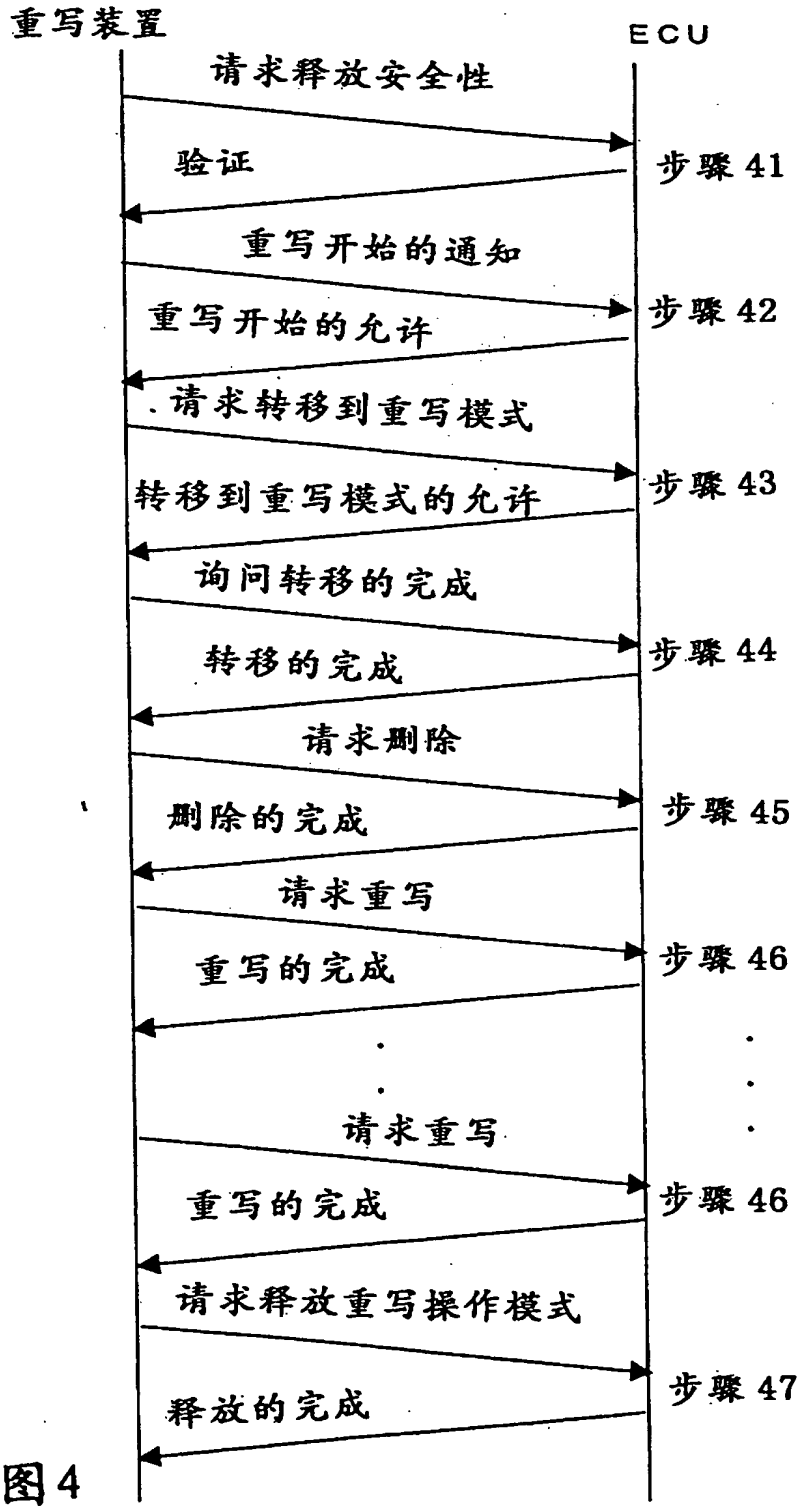

重写装置
ECU
请求释放安全性
验证
步骤 41
重写开始的通知
重写开始的允许
步骤 42
请求转移到重写模式
转移到重写模式的允许
步骤 43
询问转移的完成
转移的完成
步骤 44
请求删除
删除的完成
步骤 45
请求重写
重写的完成
步骤 46
请求重写
重写的完成
步骤 46
请求释放重写操作模式
释放的完成
步骤 47

图 4

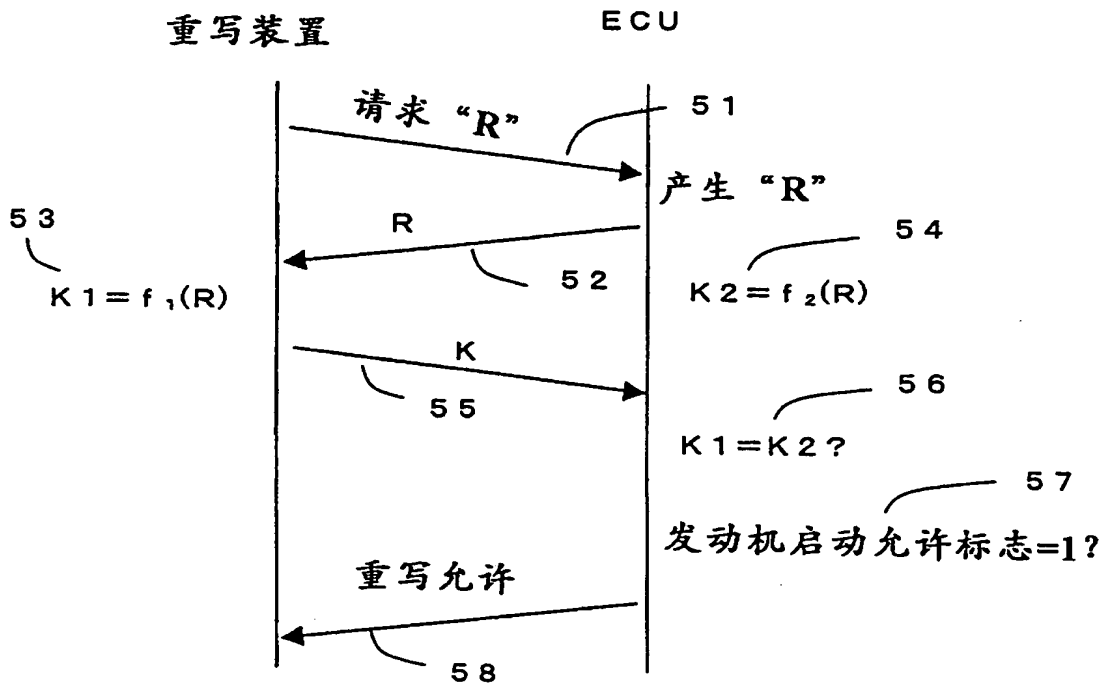

重写装置
ECU
请求 "R"
51
产生 "R"
53
R
54
52
K1=f1(R)
K2=f2(R)
K
55
56
K1=K2?
57
发动机启动允许标志=1?
重写允许
58

图5

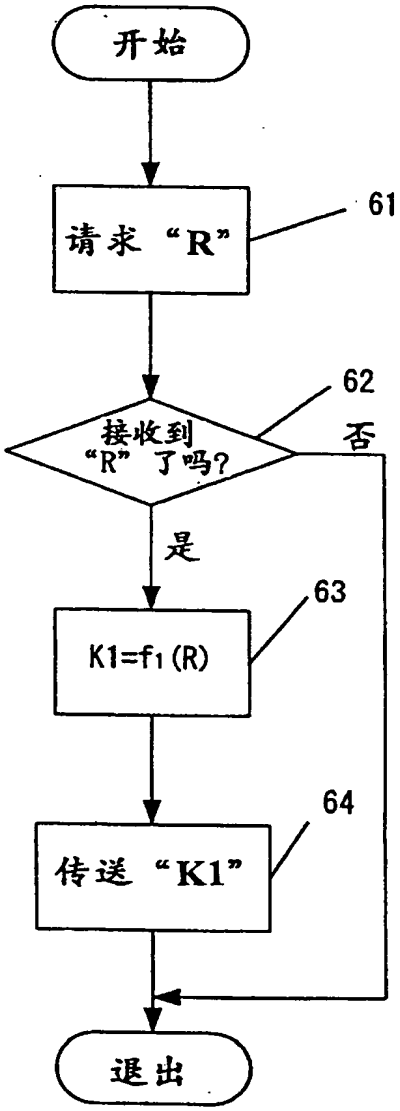


图6

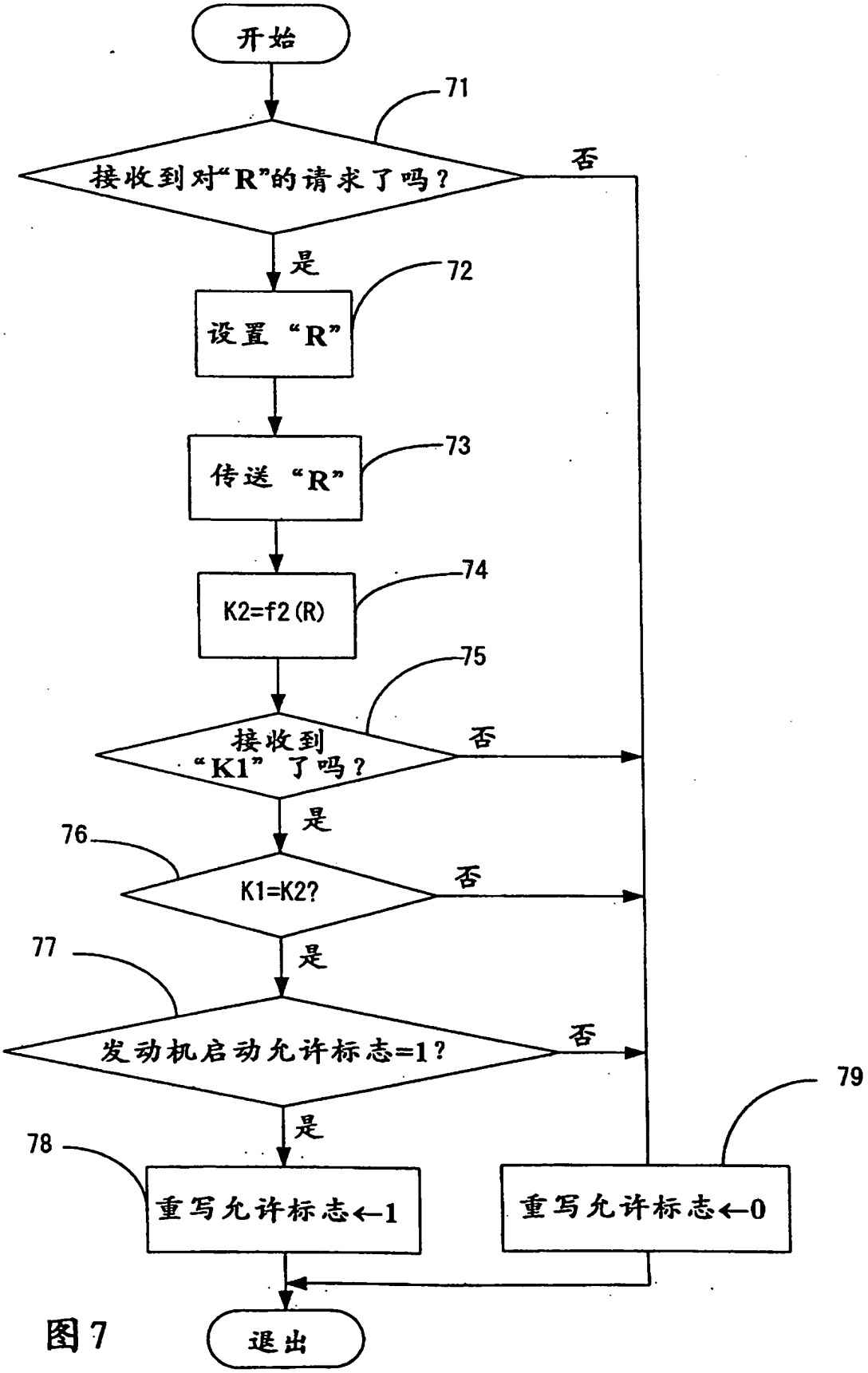

开始
71
接收到对"R"的请求了吗？
否
是
72
设置 "R"
73
传送 "R"
74
K2=f2(R)
75
接收到
"K1" 了吗？
否
是
76
K1=K2?
否
是
77
发动机启动允许标志=1？
否
是
78
重写允许标志←1
79
重写允许标志←0
退出

图 7

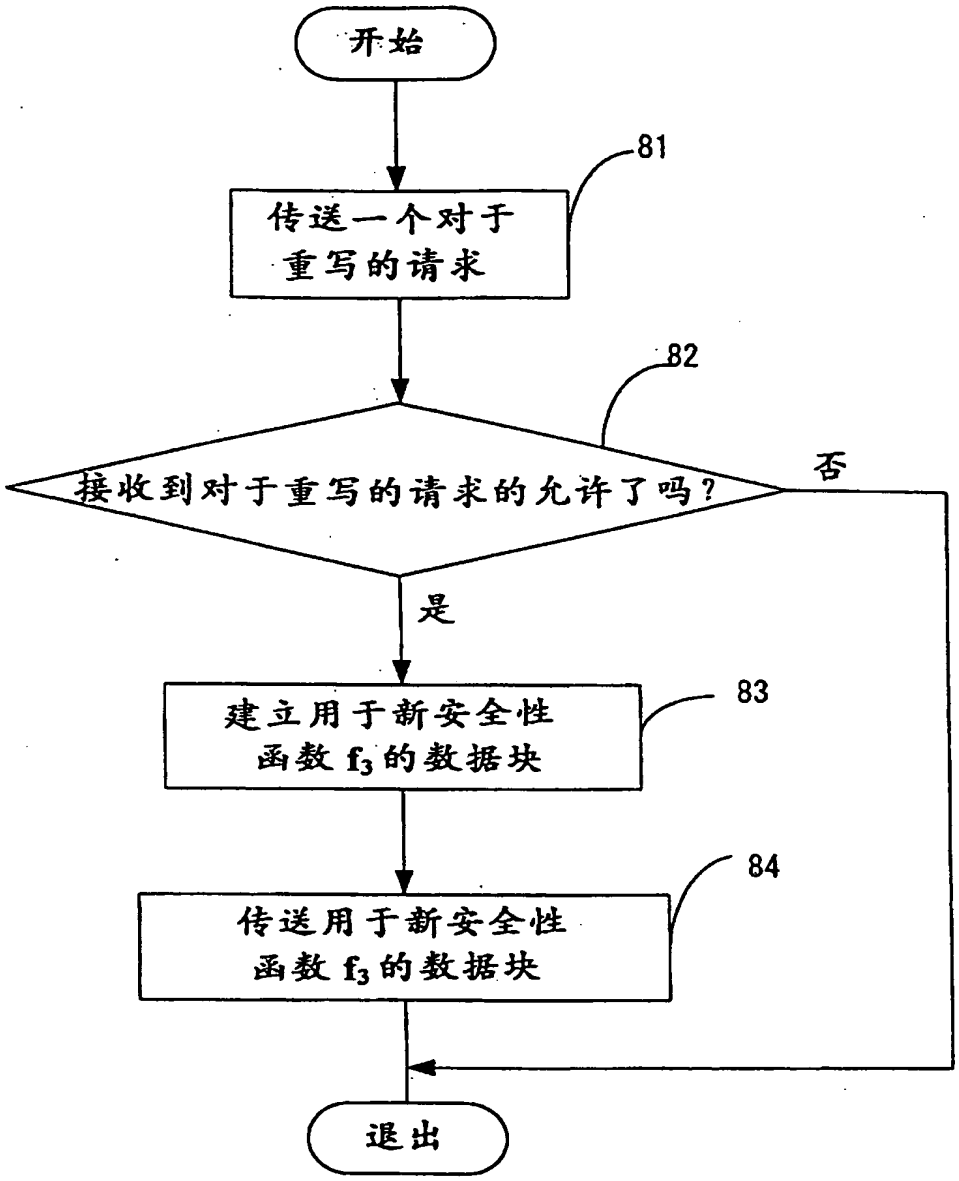

开始
81
传送一个对于
重写的请求
82
接收到对于重写的请求的允许了吗？
否
是
83
建立用于新安全性
函数 f_3 的数据块
84
传送用于新安全性
函数 f_3 的数据块
退出

图8

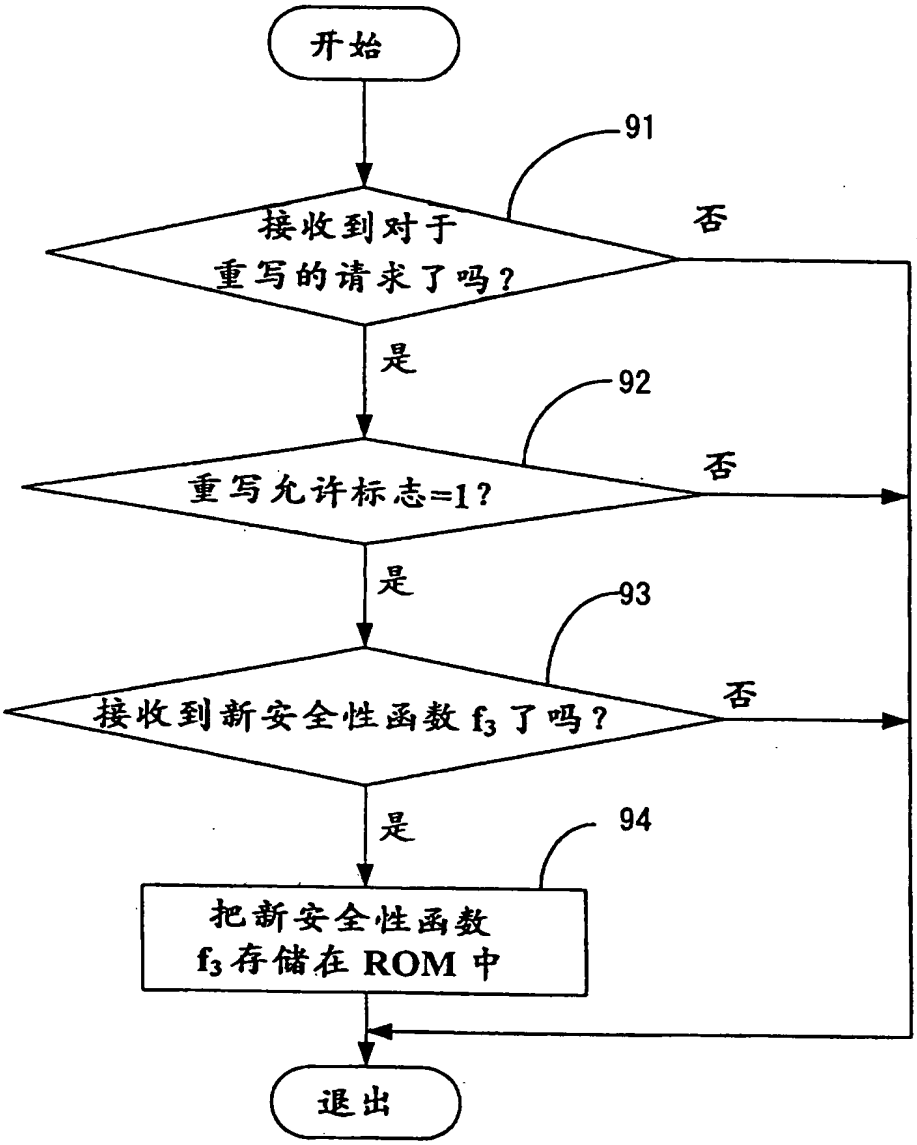

开始
91
接收到对于
重写的请求了吗？
否
是
92
重写允许标志=1？
否
是
93
接收到新安全性函数 f_3 了吗？
否
是
94
把新安全性函数
f_3 存储在 ROM 中
退出

图9